

Configure o Secure Malware Analytics Appliance com o software Prometheus Monitoring

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

Introduction

Este documento descreve as etapas para exportar dados de métricas de serviço do Secure Malware Analytics Appliance para o Prometheus Monitoring Software.

Contribuído por engenheiros do TAC da Cisco.

Prerequisites

A Cisco recomenda que você tenha conhecimento do software Secure Malware Analytics Appliance e Prometheus.

Requirements

- Secure Malware Analytics Appliance (versão 2.13 em diante)
- Licença de software Prometheus

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

TO sistema de monitoramento baseado em pesquisa Riemann/Elastic executado no Appliance é substituído pelo monitoramento baseado em Prometheus do Secure Malware Analytics Appliance versão 2.13 em diante.

Observação: o objetivo principal dessa integração é monitorar as estatísticas do seu Secure Malware Analytics Appliance usando o software Prometheus Monitoring System. Isso inclui uma interface, estatísticas de tráfego, etc.

Configurar

Etapa 1. Faça login no Secure Malware Analytics Appliance, navegue até Operations > Metrics para encontrar a chave da API e a senha de autenticação básica.

Etapa 2. Instale o software Prometheus Server: <https://prometheus.io/download/>

Etapa 3. Crie um arquivo .yml, ele deve ser chamado `dprometheus.yml` e deve ter estes detalhes:

```
scrape_configs:
- job_name: 'metrics'
bearer_token_file: 'token.jwt'
scheme: https

file_sd_configs:
- files:
- 'targets.json'

relabel_configs:
- source_labels: [__address__]
  regex: '([^/]+(/.*)?)' # capture '/.../' part
  target_label: __metrics_path__ # change metrics path
- source_labels: [__address__]
  regex: '([^/]+)/.*' # capture host:port
  target_label: __address__ # change target
```

Etapa 4. Execute o comando CLI para gerar um JWT Token para autenticação, conforme especificado no arquivo de configuração acima:

```
curl -k -s -XPOST -d 'user=threatgrid&password=<TGA Password>&method=password' "https://_opadmin
IP_:443/auth?method=password" | tee token.jwt
```

Etapa 5. Execute esse comando para verificar o campo Data de expiração do token (1 hora de validade).

```
awk -F. '{print $2}' token.jwt | base64 --decode 2>/dev/null | sed -e 's;\[^\]\]\$;\1};' | jq .
```

Exemplo de saída de comando abaixo:

```
{
"user": "threatgrid",
"pw_method": "password",
"addr": "
"exp": 1604098219,
"iat": 1604094619,
"iss": "
"nbf": 1604094619
}
```

Note: A hora é exibida no formato Epoch.

Etapa 6. Puxe a configuração dos serviços, após o login na interface opadmin, insira esta linha da interface do usuário:

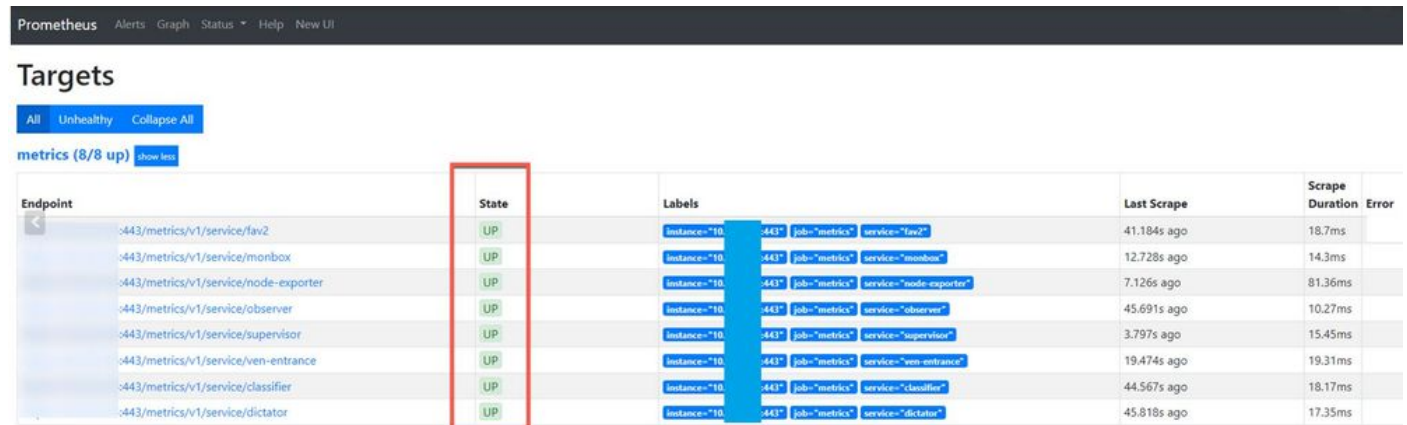
`https://_opadmin IP_/metrics/v1/config`

Passo 7. Após reiniciar o serviço Prometheus, a configuração é ativada.

Etapa 8. Acesse a página Prometheus:

`http://localhost:9090/graph`

Você pode ver os serviços Secure Malware Analytics Appliance no estado "UP", como mostrado na imagem.



The screenshot shows the Prometheus Targets page with a table of 8 targets. All targets are in the 'UP' state, indicated by green circles in the 'State' column. A red box highlights the 'State' column. The table includes columns for Endpoint, State, Labels, Last Scrape, Scrape Duration, and Error.

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
>443/metrics/v1/service/fav2	UP	instance="10", -443, job="metrics", service="fav2"	41.184s ago	18.7ms	
>443/metrics/v1/service/monbox	UP	instance="10", -443, job="metrics", service="monbox"	12.728s ago	14.3ms	
>443/metrics/v1/service/node-exporter	UP	instance="10", -443, job="metrics", service="node-exporter"	7.126s ago	81.36ms	
>443/metrics/v1/service/observer	UP	instance="10", -443, job="metrics", service="observer"	45.691s ago	10.27ms	
>443/metrics/v1/service/supervisor	UP	instance="10", -443, job="metrics", service="supervisor"	3.797s ago	15.45ms	
>443/metrics/v1/service/ven-entrance	UP	instance="10", -443, job="metrics", service="ven-entrance"	19.474s ago	19.31ms	
>443/metrics/v1/service/classifier	UP	instance="10", -443, job="metrics", service="classifier"	44.567s ago	18.17ms	
>443/metrics/v1/service/dictator	UP	instance="10", -443, job="metrics", service="dictator"	45.818s ago	17.35ms	

Verificar

Você pode ver que os dados são recebidos dos dispositivos Secure Malware Analytics Appliance e analisar as métricas com base em seus próprios requisitos, como mostrado na imagem.



Note: Este recurso funciona apenas para coletar dados específicos. O gerenciamento do fluxo de dados é de responsabilidade do servidor Prometheus.
Não há suporte para solução de problemas do Cisco TAC. Você pode contatar o suporte de terceiros para obter suporte adicional a recursos.